Title: METHOD AND APPARATUS PROVIDING SECURE
INITIALIZATION OF NETWORK DEVICES USING A
CRYPTOGRAPHIC KEY DISTRIBUTION APPROACH
Inventor: Matthew Hur

Docket No. 50325-0590    *Replacement Sheet*
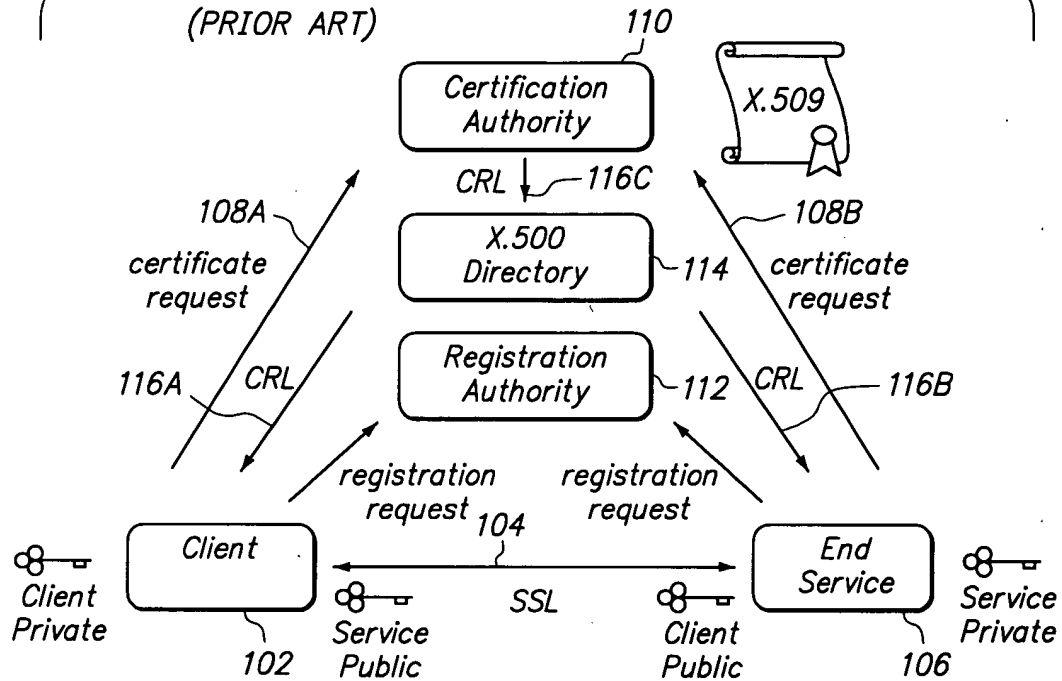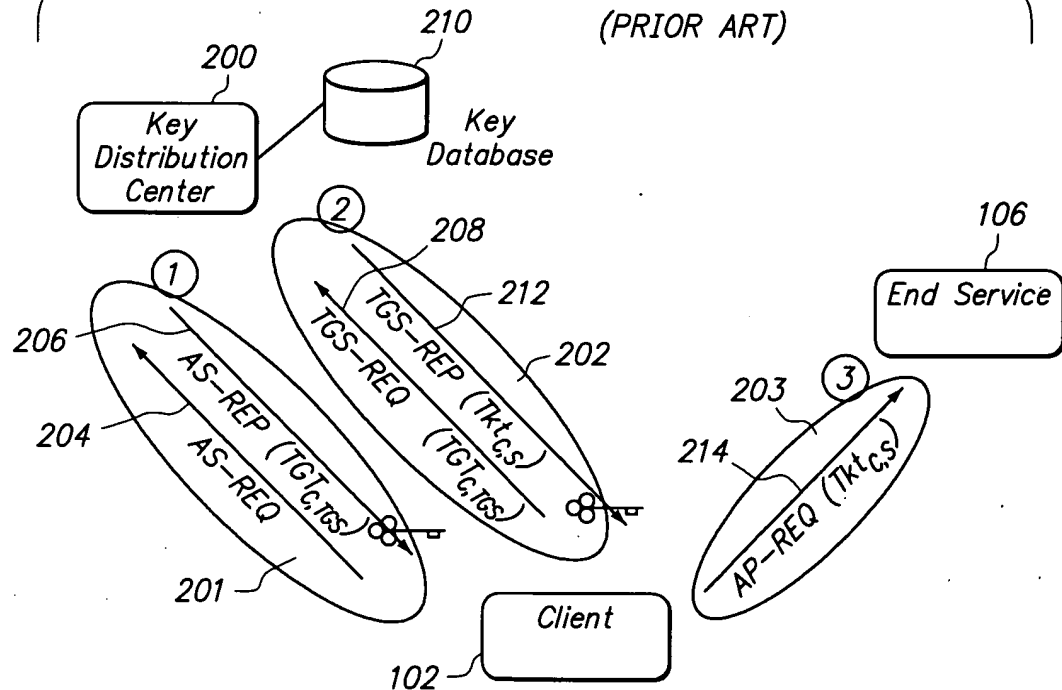
## FIG. 1
(PRIOR ART)



## FIG. 2
(PRIOR ART)

# FIG. 3A

| | |
|---|---|
| Network Device Is Manufactured, Distributed, And Deployed To End User Site | 302 |
| Network Device Is Installed At End User Site | 304 |
| Network Device Is Registered In The Network | 306 |
| Network Device Is Configured For Basic Operation And For Services Ordered By End User | 308 |
| Network Device Initiates Operation For Benefit Of End User | 310 |
| Network Device Receives Key Update(s) | 311 |

# FIG. 3B

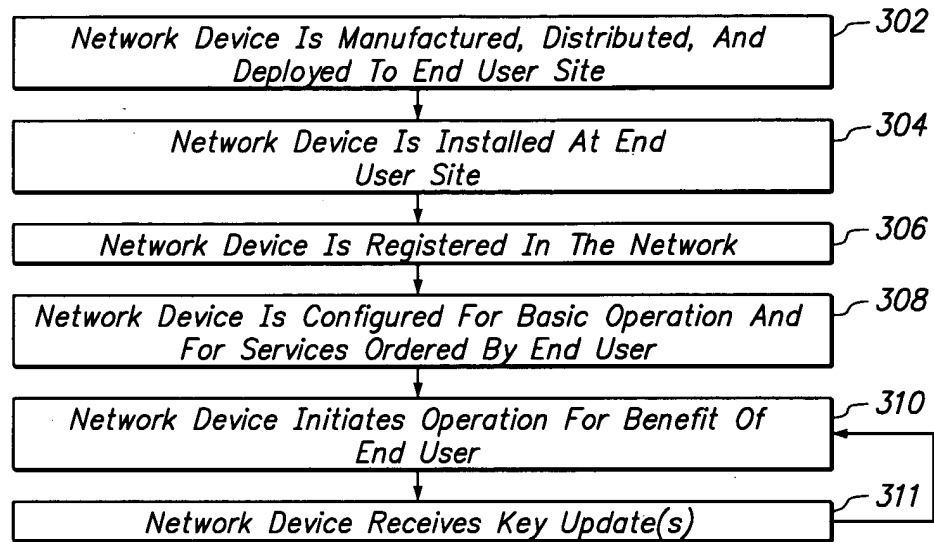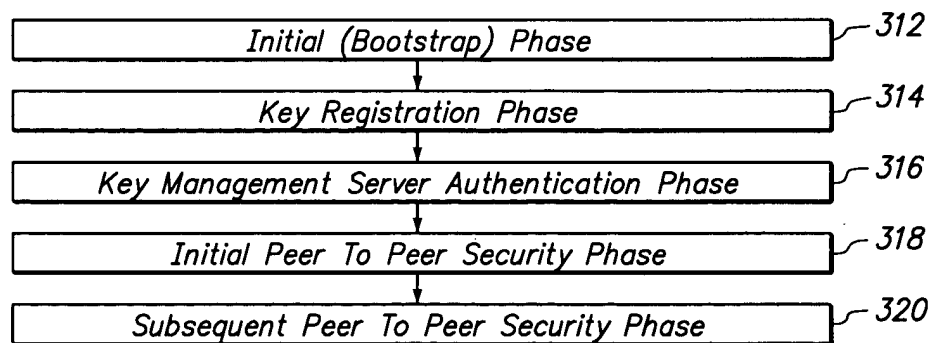| | |
|---|---|
| Initial (Bootstrap) Phase | 312 |
| Key Registration Phase | 314 |
| Key Management Server Authentication Phase | 316 |
| Initial Peer To Peer Security Phase | 318 |
| Subsequent Peer To Peer Security Phase | 320 |

Title: METHOD AND APPARATUS PROVIDING SECURE
INITIALIZATION OF NETWORK DEVICES USING A
CRYPTOGRAPHIC KEY DISTRIBUTION APPROACH
Inventor: Matthew Hur

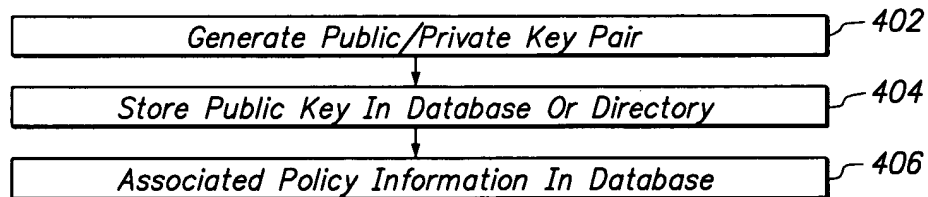Docket No. 50325-0590    *Replacement Sheet*

## FIG. 4A

| | |
|---|---|
| Generate Public/Private Key Pair | 402 |
| Store Public Key In Database Or Directory | 404 |
| Associated Policy Information In Database | 406 |

## FIG. 4B

| | |
|---|---|
| Generate Public/Private Key Pair | 410 |
| Register Public Key With A C.A. | 412 |
| Receive Public Key Certificate With Policy Information | 414 |

Title: METHOD AND APPARATUS PROVIDING SECURE
INITIALIZATION OF NETWORK DEVICES USING A
CRYPTOGRAPHIC KEY DISTRIBUTION APPROACH
Inventor: Matthew Hur

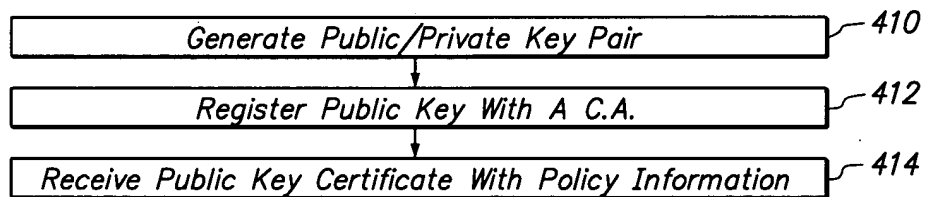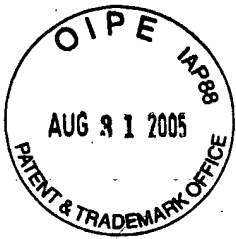Docket No. 50325-0590    *Replacement Sheet*

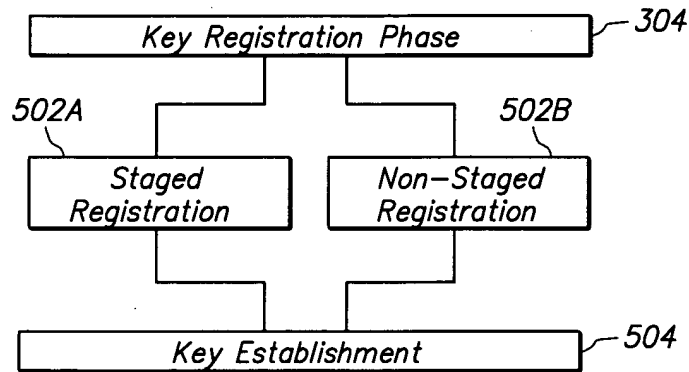## FIG. 5A

Key Registration Phase — 304

502A — Staged Registration

502B — Non-Staged Registration

Key Establishment — 504

## FIG. 5B

520 ①

key registration request

510

Device

② key registration reply    522

device private key

518

512

registration server

514

device public key

516

## FIG. 6

602 ①

ticket granting ticket request
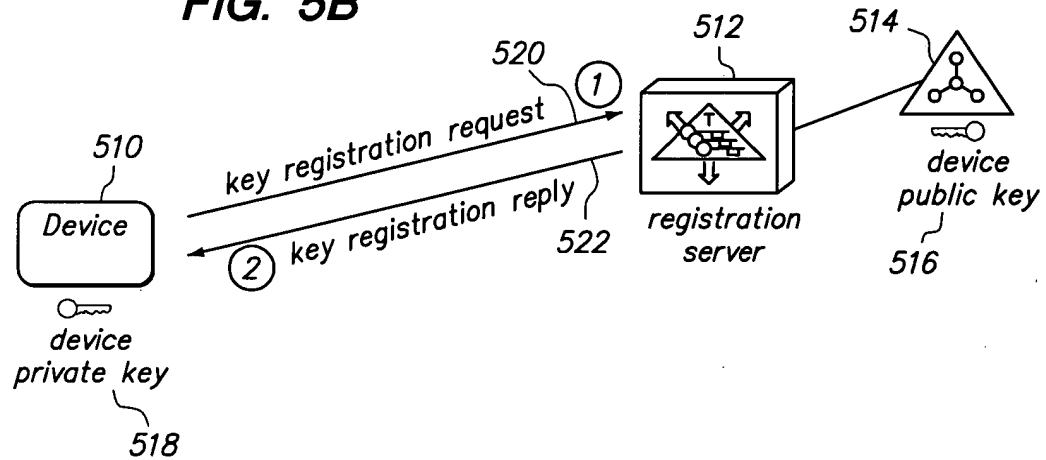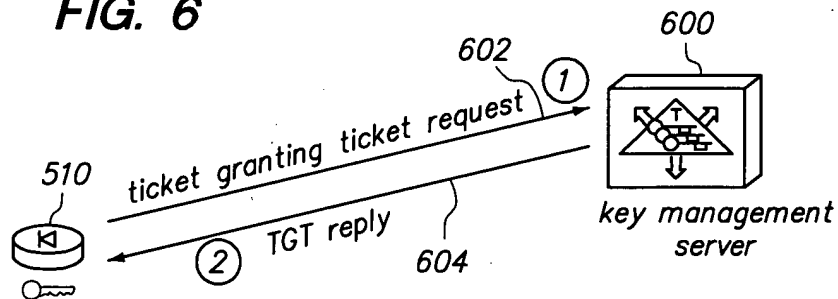
510

② TGT reply    604

600

key management server

Title: METHOD AND APPARATUS PROVIDING SECURE
INITIALIZATION OF NETWORK DEVICES USING A
CRYPTOGRAPHIC KEY DISTRIBUTION APPROACH
Inventor: Matthew Hur

Docket No. 50325-0590    *Replacement Sheet*

FIG. 7